基于贝叶斯网络的遥感云用户行为认证方法 *

成路肖 [1]，阎继宁 [2]，焦　阳 [1]，马　艳 [3†]，王玉柱 [4]

(1. 燕山大学 信息科学与工程学院, 河北 秦皇岛 066004; 2. 中国地质大学(武汉) 计算机学院, 武汉 430074; 3. 中国科学院遥感与数字地球研究所, 北京 100094; 4. 中国地质大学(北京) 信息工程学院, 北京 100083)

摘　要：针对遥感云服务平台中不可信用户的入侵现象，结合遥感云用户行为特点和贝叶斯网络算法设计了一种用户行为认证方案。该方案论述了遥感云平台用户的行为认证机制，并且根据用户行为特点建立了用户行为认证集，结合贝叶斯网络算法预测特点和用户行为属性建立了用于认证等级预测的贝叶斯网络模型，把该模型中分析得出的用户行为属性的权重信息应用到用户等级预测算法中，使该算法针对遥感云用户认证更安全准确，从而实现对用户行为认证等级的预测。仿真实例表明该方法能够准确识别出不可信用户，有效保证遥感云服务平台的安全性。

关键词：用户行为认证；贝叶斯网络；遥感云服务平台；行为分析；云计算

中图分类号：TP393　　doi: 10.3969/j.issn.1001-3695.2017.09.0903

Bayesian network method for remote sensing cloud user behavior authentication

Cheng Luxiao[1], Yan Jining[2], Jiao Yang[1], Ma Yan[3†], Wang Yuzhu[4]

(1. *School of Information Science & Engineering*, *Yanshan University*, *Qinhuangdao Hebei* 066004, *China*; 2. *School of Computer Science*, *China University of Geosciences*, *Wuhan* 430074, *China*; 3. *Institute of Remote Sensing & Digital Earth*, *Chinese Academy of Sciences*, *Beijing* 100094, *China*; 4. *School of Information Engineering*, *China University of Geosciences*, *Beijing* 100083, *China*)

Abstract: Aiming at the intrusion of untrusted users in remote sensing cloud platform, this paper designed a user behavior authentication scheme based on the characteristics of remote sensing cloud user behavior and Bayesian network algorithm. The scheme discussed the users' behavior authentication mechanism of remote sensing cloud platform, and according to the users' behavior characteristics, the scheme established an authentication set on users' behavior. Combining with the predictive characteristics of bayesian network algorithm and user behavior properties to set up a Bayesian network model for authentication grade prediction. The weight information of user behavior attributes analyzed in this model is applied to the user grade prediction algorithm, which made the algorithm more secure and accurate for remote sensing cloud user authentication safer accurately, so as to realize the prediction of user behavior authentication level. Simulation examples show that the model is effective to identify untrusted users accurately, and can ensure the security of remote sensing cloud platform.

Key Words: user behavior authentication; Bayesian network; the remote sensing cloud platform; behavior analysis; cloud computing

0　引言

近年来，在人们享受着云计算带来的高效率、低成本的同时，也面临着严峻的信息安全挑战。遥感云服务平台是基于云计算技术，将遥感数据、信息产品、处理算法技术与计算资源打包成可计量的服务，用户可以通过网络按照个人需求和自身爱好获得相应的应用及服务资源[1]，主要包括多源遥感数据分发共享、高性能数据处理及产品生产、云存储、遥感计算平台供给等服务。然而，由于用户是对云服务提供者提供的软件环境、网络基础性设施和计算平台等进行直接操作，所以攻击者对云资源软硬件的影响和破坏远比利用因特网进行共享资源要严重的多，例如 IaaS（instrument as a service,基础设施即服务），服务商提供的是一个包含一些组件和功能的共享设施，如存储、操作系统和服务器等对于该系统的使用者而言并不是完全隔离

基金项目：国家“863”计划资助项目（2013AA12A301）；国家重点研发计划项目（2016YFB0200800）；国家自然科学基金资助项目（61602477）

作者简介：成路肖（1989-），女，硕士研究生，主要研究方向为云计算环境下的用户行为特征；阎继宁（1986-），男，特任副教授，博士，主要研究方向为高性能空间数据处理、遥感云计算；焦阳（1991-），男，硕士研究生，主要研究方向为遥感大数据集成与管理；马艳（1983-），女（通信作者），副研究员，博士，主要研究方向为高性能地学计算、空间大数据、云计算（mayan@radi.ac.cn）；王玉柱（1988-），男，讲师，博士，主要研究方向为高性能地学计算、云计算、大数据.

的，当遭受攻击时，全部服务器对攻击者将会是透明的[2]。又如当用户访问云存储服务时,首先需要进行身份认证保证访问用户身份的正确性和合法性。只有对用户身份实现安全正确的认证，才能确保后续访问和使用遥感云服务的对象是合法用户,但是合法的登陆用户也不保证是安全的用户，因此用户行为是否可信，如何对云端用户行为可信度进行评估预测是当下保证云计算安全的重要内容。

云计算的应用领域中，很多学者研究了用户行为信任评估方法在云计算环境下的应用问题，例如文献[3]提出一种行为信任预测的博弈控制机制，首先利用贝叶斯网络对用户的行为信任进行预测，然后根据预测结果和博弈分析相结合，推导出了一种纳什均衡策略。文献[4]提出一种根据用户行为和平台环境特征评估信任级别的方法。文献[5]提出一种基于动态信任管理的云安全认证服务机制，将 PKI 技术和动态信任管理方法相结合实现云环境下的安全认证。文献[6]提出一种基于用户鼠标行为的身份认证方法，采用层次结构的分类决策模型对用户身份进行认证。但是该认证机制的制定并不能针对一个特定的云计算服务平台。以上的这些模型都部分解决了在不同应用背景下用户信任及评估等问题，但是每个模型和方法的训练集提取具有针对性，所以这些模型都缺乏灵活的信任评价机制，无法满足不同领域用户行为评估时所具有的个性化特点。

本文针对遥感云服务平台用户行为特征在传统的身份认证基础上结合行为认证机制，提出一种基于贝叶斯网络模型的用户行为认证方法。

1　遥感云服务平台

遥感云服务平台，基于云计算技术，整合各种遥感信息和技术资源，将遥感数据、信息产品、应用软件、计算及存储资源作为公共服务设施，通过网络为用户提供一式站的空间信息云服务。遥感云服务平台基于 OpenStack 云计算框架开发，其系统架构从下到上大致分为五层，分别是资源层、管理层、计算层、业务层和服务层，如图 1 所示。其中资源层通过虚拟机管理程序将大量用网络连接的计算资源、网络资源和存储资源构建成虚拟化资源池，形成遥感云系统内部可以统一管理的虚拟 CPU、虚拟内存、虚拟磁盘、虚拟对象存储空间及虚拟网络等虚拟资源。管理层主要采用 OpenStack 计算框架，利用其核心组件实现对虚拟资源的管理。计算层主要提供虚拟集群计算环境，包括海量遥感数据存储、集群计算和调度、计算环境监控等服务。业务层主要包括多中心遥感数据管理、遥感数据处理及产品生产高性能计算平台两部分。此外，基于 SaltStack 管理工具等还可以实现虚拟计算环境的自动部署与系统扩容。最终实现的遥感云原型系统主界面如图 2 所示，为用户提供的服务括：遥感数据服务、信息产品服务、遥感数据处理服务、云平台服务、云存储服务。其中遥感数据服务指多源遥感数据的采集、存储、检索、下载等；信息产品服务指遥感信息产品的生产和分发服务[7]；遥感数据处理服务基于 MPI 并行计算机机制，可以根据用户提交的数据处理需求实现海量遥感数据的高性能在线处理，并可以根据计算任务量扩展计算资源；云平台服务负责根据用户提出的虚拟遥感计算环境的需求，为用户创建虚拟计算资源、定制遥感计算模板实例或个性化实例；云存储服务主要满足遥感云数据存储的需求，并且可以根据需求对自己的云存储进行动态扩容。

此外，为保证遥感云服务平台的安全性，除了在资源层部署防火墙、在计算层进行虚拟计算集群监控外，还需要在业务层之上进行用户行为特征监控。

一般对于一个特定的系统或服务平台而言，每个用户的行为状态和操作习惯都遵循一定的规律。例如遥感云平台中合理的行为轨迹包括标准遥感数据及遥感产品的检索、浏览、订购、下载和转存[9]，然后利用遥感云高性能遥感数据处理及产品生产平台进行在线数据处理及产品生产，或者在线定制个人遥感虚拟计算环境进行数据处理，并将最终的处理结果存入个人云存储。当用户行为异常时则需要对用户行为进行认证，认证不通过则拒绝提供服务。

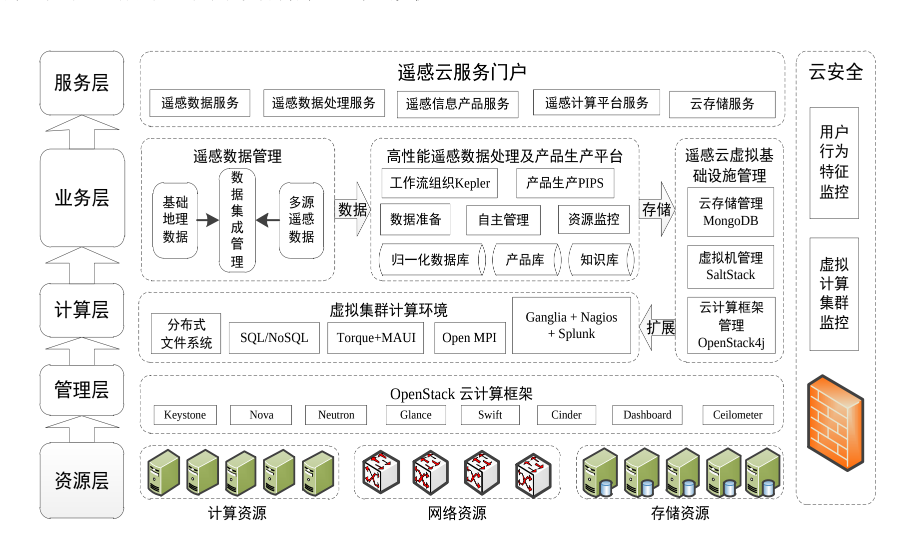


图 1　遥感云服务平台体系架构



图 2　遥感云服务平台主界面

2　用户行为认证方案

用户行为认证包括身份认证和行为认证两部分。根据遥感云用户个性化行为特征，设计出更细粒度的行为信任认证方案。行为认证的设计思路是：将服务器日志和客户端数据相结合的方法提取出用户行为数据信息，包括通过 Web 日志获取用户浏览过和订购过的数据及服务信息，并且通过服务器日志获取用户进入遥感云平台的浏览行为记录等。用户在提交系统访问请求时需要先进行身份认证，若身份认证失败，则直接拒绝提供服务；若用户身份认证成功，则进入到行为认证阶段。行为认证指服务器获取用户实时行为证据，将行为证据与存储在数据库中的行为认证集进行匹对验证[8]。在行为认证过程中，根据行为证据定位到特定的行为认证集，结合实时行为证据采用贝叶斯网络(Bayesian network)计算每个行为认证集信任等级，最后根据决策算法计算出用户行为信任等级。遥感云服务平台用户行为认证方案具体流程如图 3 所示。详细步骤如下：

a) 当终端用户向服务器发送服务请求时，行为认证机制首先进行身份认证，对于身份认证成功且不是首次登录的用户，允许访问并且实施实时行为监控，执行步骤 b)；对于身份认证成功且是首次登录访问云平台的用户，允许授权访问，实施重点行为监控，执行步骤 d)；对于身份认证失败的用户，则拒绝服务访问。

b) 获取用户行为状态信息，进行基于行为状态认证集的认证，对于状态认证不成功的拒绝其访问；对于通过状态认证集认证的用户，允许授权访问，执行步骤 c)。

c) 查找用户历史行为认证信息，如果用户历史行为认证状态为“一般可信”则进入预警防范，允许授权访问，但是要进行重点实时行为监控，执行步骤 d)；如果历史行为认证状态为“不可信”，则拒绝访问。

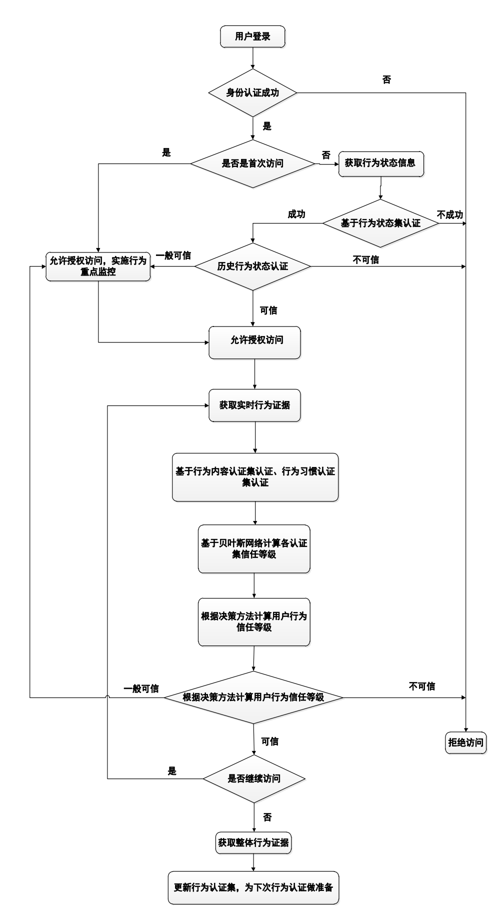


图 3　用户行为认证流程

d) 获取用户实时行为证据，实现行为内容认证集和行为习惯认证集的认证，根据贝叶斯网络模型计算出各行为认证集的信任等级，最后根据决策方法计算出用户行为信任等级，若“可信”且继续访问，执行步骤 b)；若“可信”或“一般可信”且终止访问，则执行步骤 e)；若“一般可信”且继续访问，则允许访问并且实施行为重点实时监控，执行步骤 b)；若“不可信”，则终止用户访问。更新用户行为认证集及用户历史可信认证状态信息。更新用户行为认证集及用户历史可信认证状态信息。

e) 更新用户行为认证集及用户历史可信认证状态信息。

2.1　用户行为认证集

用户行为认证集具有个性化的特点，并且对保证行为认证的准确性至关重要，因此确定行为认证集是行为认证过程中非常重要的内容之一[9]。认证过程中需要获取实时用户行为证据与用户行为认证集进行对比，用户行为认证成功的概率取决于行为认证集的划分、定义和行为相关的集合覆盖率。

用户行为认证集包含以下几个方面：行为状态认证集(SA)、行为内容认证集(CA)、行为习惯认证集(HA)。其中行为状态认证集是由引发行为状态异常的行为属性构成，如用户登录地点、客户端 IP 地址、操作系统版本和访问时间突然与历史行为状态不一致导致的行为状态异常。其中 PaaS 层和 SaaS 层的行为状态异常检验都需要对照操作系统、IP 地址和访问的时间这几个证据属性，IaaS 层只提供基础设施服务，因此不需要对客户端的操作系统这一证据属性进行认证。行为内容主要包括用户资源的使用情况，如资源使用的种类和数量等。在云计算环境的不同服务模式下，资源的内容不同，在 IaaS 层主要指处理、存储、网络等基础性的计算资源，在 PaaS 层指服务器、操作系统、中间件等开发环境，正常情况下，终端用户使用资源的数量、种类不会有很大变化，如果出现了较大的变化，则有可能用户的行为出现异常，需要进行行为认证[10]。特别在 SaaS 服务模式中，不同的终端用户其具体的行为内容是不一样的。行为习惯主要包括用户经常访问的网站，习惯进入资源的页面引用和习惯访问的资源等。

2.2　用户行为认证过程

用户行为认证过程包括下列三个主要过程：

a) 行为前的用户身份认证、行为状态认证。

b) 行为中的实时动态状态认证，包括行为状态认证、行为内容认证、行为习惯认证。

c) 行为后的证据认证集更新，为下一次的行为认证做准备。

用户认证机制如图 4 所示。具体步骤为：

a) 通过客户端获取用户实时行为，并将行为证据通过网络传输到用户行为认证服务器端；

b) 用户行为认证服务器对捕获到的用户行为进行认证；

c) 通过服务器进行行为认证集的行为认证；返回行为认证集的认证结果；

d) 返回认证结果；

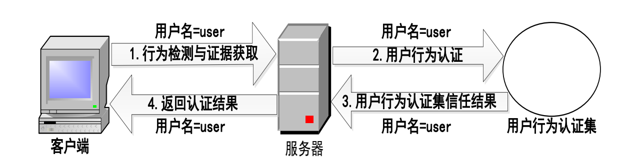


图 4　用户行为认证机制

用户在访问系统时首先进行身份认证，若用户的身份不可信，则直接拒绝提供服务；若用户的身份可信且非首次访问，则进入到行为认证阶段；若用户身份可信并且是首次访问，则允许授权访问，进行重点实时行为监控。行为认证就是将用户和系统在交互中获取的实时行为证据提交给相应的服务器，服务器将提交的行为证据与存储在数据库中的用户行为认证集进行匹对，根据认证结果确认用户行为是否可信[10]，若认证结果可信则向用户提供信息服务，若不可信则拒绝提供信息服务。

3　用户行为信任等级预测

3.1　用户行为信任预测的贝叶斯网络模型

用户行为信任预测是基于用户的历史交往行为证据之上，结合用户当前的实时行为，对用户进行信任等级预测。贝叶斯网络是一个有向无环图，它由代表变量的节点及连接这些节点的有向边组成[11,13]，构成用户行为信任等级预测的贝叶斯网络模型见

如图 5 所示，变量节点包括要预测的用户各行为认证集及其包含的行为属性集，其中行为认证集包括行为状态认证集简称 SA、行为内容认证集简称 CA、行为习惯认证集简称 HA。行为认证集的子节点是对应的用户行为属性，如用户行为状态认证集 SA 及其包含的行为属性有客户端信息、IP 信息、登录信息等；用户行为内容认证集 CA 及其包含的行为属性有遥感数据处理软件使用类型、下载遥感数据数量、订购遥感产品种类、订购遥感虚拟计算环境类型（农业专题、林业专题、矿产专题、海洋专题等）；用户行为习惯认证集 HA 及其包含的行为属性有常访问的遥感云服务类型、常下载的遥感数据或产品类型、常订购的遥感虚拟计算环境类型、页面引用等。贝叶斯网络可以将用户行为信任等级预测和用户行为属性用有向图直观的表示出来[3]，同时将用户历史和实时行为统计数据以条件概率的形式融入模型，这样将用户行为的先验知识和后验数据无缝的结合在一起，并且贝叶斯网络中的各节点之间是相互影响的，任何节点的值的改变都会影响其他节点，因而能满足不同需求细粒度组合的推理和预测效果。

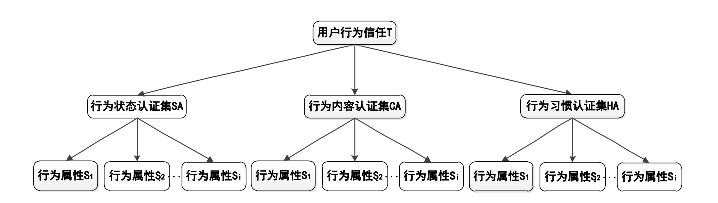


图 5　用户行为信任预测的贝叶斯网络模型

3.2 用户行为属性等级的先验概率

在利用贝叶斯网络进行用户行为认证时，需要先计算出用户行为属性的先验概率。本文将用户行为信任 T、行为状态 SA、行为内容 CA、行为习惯 HA 以及各行为认证集对应的行为属性等节点划分为 L 个信任等级，并对这些信任等级从高到低赋予编号 $i(i=1,2,3\ldots.L)$。数组下标表示不同的取值范围，因此 T_i、SA_i、CA_i、HA_i 、S_i 分别表示整体行为信任、行为状态认证集、行为安全认证集、行为习惯认证集和行为属性的范围。$|T_i|$、$|SA_i|$、$|CA_i|$、$|HA_i|$、$|S_i|$分别表示预测用户交往历史中整体信任、各行为认证集和行为属性的值分别落在 T_i、SA_i、CA_i、HA_i 、S_i 范围内的次数。n 表示交往总次数，$P(T_i)$、$P(SA_i)$、$P(CA_i)$、$P(HA_i)$、$P(S_i)$分别表示他们的概率，这些符号的含义在全文中都适用。

用户行为认证集等级的先验概率计算公式如下：

$$p(T_i)=\frac{|T_i|}{n}(1\le i\le 3),\text{并且}\sum_{i=1}^{3}\mathrm{p}(\mathrm{T_i})=1 \tag{1}$$

计算用户行为属性集等级的先验概率，其计算方法与计算用户行为认证集等级的先验概率的方法类似。行为属性信任等级的先验概率 $P(S_i)$为

$$p(S_i)=\frac{|S_i|}{n}(1\le i\le L),\text{并且}\sum_{i=1}^{L}\mathrm{p}(\mathrm{S_i})=1 \tag{2}$$

3.3 行为认证集的条件概率

除了计算先验概率外，还需要各行为认证集等级的条件概率。认证集等级的条件概率计算公式如下：

$$p(e/h)=\frac{p(h,e)}{p(h)} \tag{3}$$

它表示在满足 h 的条件下满足 e 条件的概率。以计算 $p(S_i|CA_j)$条件概率为例，它表示行为内容认证等级为 j 的条件下，行为属性节点落在 S_i 范围内的概率，其计算公式如下：

$$P(S_i|CA_j)=\frac{P(S_i,CA_j)}{P(CA_j)}=\frac{|S_i\ I\ CA_j|/n}{|CA_j|/n}=\frac{|S_i\ I\ CA_j|}{|CA_j|} \tag{4}$$

由以上计算方法得到的各个行为属性集等级的先验概率和条件概率可以得到行为认证集信任等级的概率。下面在单行为属性条件下，以预测行为内容认证集信任等级为例，其他行为认证集计算方法与此类似。计算行为内容认证集中行为属性节点落在 S_j 范围内的条件下，行为内容认证等级为 i 的概率 $P(CA_i|S_j)$。利用贝叶斯公式得

$$\begin{aligned}P(CA_i|S_j)&=\frac{P(S_j|CA_i)P(CA_i)}{p(S_j)}\\&=\frac{(|S_j\ I\ CA_i|/|CA_i|)(|CA_i|/n)}{|S_i|/n}\\&=\frac{|C_j\ I\ CA_i|}{|S_j|}\end{aligned} \tag{5}$$

对于多个行为属性条件下，以预测行为内容认证集为例，其他行为认证集信任等级预测类似。假设有行为内容认证集包含四个行为属性分别为 $S1$、$S2$、$S3$、$S4$，分别落在 $S1_j$、$S2_k$、$S3_m$、$S4_n$ 的条件下，行为认证集 CA 信任等级的预测，计算公式如下：

$$\begin{aligned}\mathrm{p}(\mathrm{CA_i}|\mathrm{S1_j},\mathrm{S2_k},\mathrm{S3_m},\mathrm{S4_n})&=\frac{\mathrm{p}(\mathrm{S1_j},\mathrm{S2_k},\mathrm{S3_m},\mathrm{S4_n}|\mathrm{CA_i})\mathrm{p}(\mathrm{CA_i})}{\mathrm{p}(\mathrm{S1_j},\mathrm{S2_k},\mathrm{S3_m},\mathrm{S4_n})}\\&=\frac{(|\mathrm{S1_j\ I\ S2_k\ IS3_m\ I\ S4_n}|/|\mathrm{CA_i}|)(|\mathrm{CA_i}|/\mathrm{n})}{|\mathrm{S1_j\ I\ S2_k\ IS3_m\ I\ S4_n}|/\mathrm{n}}\\&=\frac{|\mathrm{S1_j\ I\ S2_k\ IS3_m\ I\ S4_n\ I\ CA_i}|}{|\mathrm{S1_j\ I\ S2_k\ IS3_m\ I\ S4_n}|}\end{aligned} \tag{6}$$

3.4 行为信任等级的计算方法

在计算出每个行为认证集的信任等级后，然后根据图形化的贝叶斯网络分析出各行为认证集的权重信息，最后根据多项式的计算方法得出用户行为信任等级 T 为

$$T=\sum_{i=1}^{i}C_iW_i\quad(W_i\ge 0,\sum_{i=1}^{i}W_i=1) \tag{7}$$

其中：C_i 代表第 i 个行为认证集的信任等级，W_i 代表第 i 个行为认证集的权重。

4 认证方法安全性分析

安全性是认证方法中最重要的问题。该行为认证方案的安全性主要体现在两个方面：①从整个认证流程上分析，针对不同情况给出了更具体的策略，对于通过身份认证的用户，对其每个行为请求都进行行为信任预测，如超出可信范围则拒绝该用户的行为请求操作，在认证流程上保证了认证的安全性。②从认证算法上分析，通过用户行为构建的贝叶斯网络模型分析出的行为属性权重信息，将该行为属性权重信息和贝叶斯网络算法相结合，避免了算法的主观性和不确定性，使该算法更具有针对性，针对该平台更具有安全性，能够更准确的预测出遥感云平台恶意行为用户，保证整个认证过程的安全性。

5 用户行为信任等级预测实例与分析

根据以上提出的用户行为信任等级预测方法，下面将通过一个实例来演示预测模型的有效性。根据用户 U 与遥感云服务平台的交互统计 207 组数据，某时刻，用户 U 请求访问服务器 S，现通过模型预测在某些特定行为属性认证集的条件下用户 U 的行为信任等级。行为信任划分为三个等级：信任、一般信任、不信任。下面给出该用户的行为内容信任等级预测过程。其中该用户行为证据落在不同行为属性区间频数（$S1$、$S2$、$S3$ 代表三个不同的行为属性）见表 1。

1)行为认证集信任等级的计算

根据上面得到的用户行为交互数据信息，利用式(2)可以计算出网络中各节点的先验概率，其行为属性节点的先验概率见表 2，同理行为认证等级节点 T 的条件概率表见表 3。再由式(4)计算出各证据属性的条件概率，得出每个证据属性的条件概率表 CPT。得出了所有节点的先验概率和子节点的条件概率，这样在计算行为认证集的信任等级预测的时候，对于任意一组观测值都有相应的先验概率和条件概率，分别将其带入式(5)就

可以得到所有的后验概率，最后取最大概率值作为每个行为认证集的信任等级。

表 1　用户行为证据落在行为属性集区间的频数

范围	S1 频数	范围	S2 频数	范围	S3 频数
S11	33	S21	47	S31	36
S12	73	S22	98	S32	89
S13	101	S23	62	S33	82

表 2　行为属性节点的先验概率

节点	先验概率	节点	先验概率	节点	先验概率
S11	33/207	S21	47/207	S31	36/207
S12	73/207	S22	98/207	S32	89/207
S13	101/207	S23	62/207	S33	82/207

表 3　行为认证节点的先验概率

T	P(T)
1	1/3
2	1/3
3	1/3

2)用户行为信任等级的计算

根据上面提到的用户行为信任等级的预测步骤，利用贝叶斯网络模型分析得出各行为属性的贝叶斯网络结构关系图，如图 6 所示。从该贝叶斯网络结构图中分析出每个行为属性对最后用户行为信任等级预测的权重信息。该实验中用户行为属性权重分布图如图 7 所示，得出的各个行为属性的权重值分别为：页面引用权重为 0.225，浏览地址 URL 权重为 0.190，访问时间权重为 0.190，字节数权重为 0.165，使用资源权重为 0.225，客户端信息权重为 0.072。根据行为属性的权重值，利用加权平均的算法计算出每个行为认证集的权重值，该实验得出的行为状态认证集的权重分别为：行为状态认证集权重 W_s=0.392，行为内容认证集权重 W_c=0.402，行为习惯认证集权重 W_h=0.206。



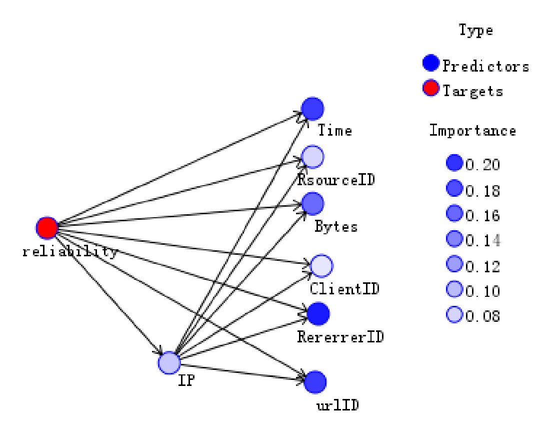


图 6　贝叶斯网络分析结构

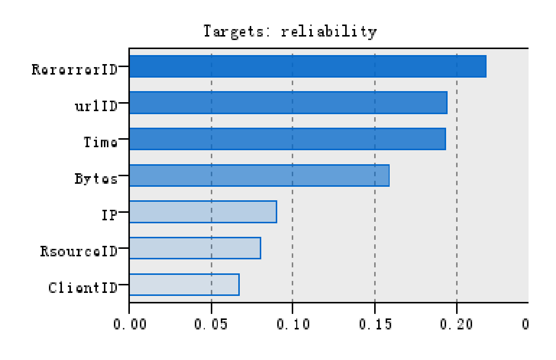


图 7　行为属性权重分布图

本次会话结束后，根据分析出的权重值利用式(7)计算出用户 U 最终预测的行为信任等级为 2“一般可信”。在结束本次会话后，更新行为证据数据库，为下一次用户行为认证做准备。同时，当该用户继续访问时，则对他的每个操作行为请求重新认证，以确保该用户行为的可信性，保证用户的安全性。

该实验根据遥感云服务平台用户行为特点建立了三种用户行为认证集。根据贝叶斯网络条件独立性假设特点及行为认证与行为属性之间的因果关系建立预测用户行为信任等级的贝叶斯网络模型，根据模型可以对用户行为进行细粒度的用户行为认证集的信任等级预测。文中利用贝叶斯网络分析出用户行为属性对信任等级预测结果的权重信息，最后利用决策方法计算出用户信任等级。

6　结束语

用户行为是云计算环境下网络安全领域研究的重要方向，在用户行为认证中身份认证是整个信息安全的基础。但是传统的身份认证无法阻止合法用户的恶意行为入侵。本文论述了基于贝叶斯网络的遥感云服务平台用户行为认证过程，融合了贝叶斯网络推理技术来求解用户行为信任等级问题，在身份认证的基础上结合贝叶斯网络模型实现了用户行为认证。贝叶斯网络推理技术把行为信任等级问题根据变量与属性之间的因果依赖关系进行了分解。由于贝叶斯网络的条件独立假设特征，使得贝叶斯网络推理技术求解问题时只需要考虑当前节点与其父节点之间的关系，简化计算并且有利于准确地估算概率分布，提高预测的准确性。但是这类方案在以后也会面临不少攻击，由于研究与使用的经验缺乏,其面临的攻击以及防御攻击的可行性方案还需要进一步研究。

参考文献：

[1] 李小宁，李磊，金连文，等. 基于 OpenStack 构建私有云计算平台 [J]. 电信科学, 2012, 28 (9): 1-8.

[2] Reichert A. PaaS 的未来、应用及其安全性. [EB/OL]. (2014-9-02) [2017-09-05]. https://searchcloudcomputing. techtarget. com. cn/5-10646/.

[3] 田立勤，林闯. 可信网络中一种基于行为信任预测的博弈控制机制 [J].

计算机学报, 2007, 30 (11): 1930-1938.

[4] 邹冰玉，张焕国，郭曦，等. 可信网络连接中一种基于可信度的细粒度授权模型 [J]. 武汉大学学报：理学版, 2010, 56 (2): 147-150.

[5] 朱莉蓉，陈宁江，何佩聪，等. 基于动态信任管理的云用户行为认证服务系统 [J]. 广西大学学报：自然科学版, 2015, 40 (6): 1485-1493.

[6] 徐剑，李明洁，周福才，等. 基于用户鼠标行为的身份认证方法 [J]. 计算机科学, 2016, 43 (2): 148-154.

[7] 李良，田立勤，李君建. 云计算环境下用户行为的认证与预测 [J]. 计算机系统应用, 2016, 25 (6): 125-130.

[8] 陈亚睿. 云计算环境下用户行为认证与安全控制研究 [D]. 北京：北京科技大学, 2012.

[9] 陈亚睿，田立勤，杨扬. 云计算环境下动态用户行为认证的机制、模型与分析 [J]. 系统仿真学报, 2011, 23 (11): 2302-2307.

[10] 赵洁，肖南峰，钟军锐. 基于贝叶斯网络和行为日志挖掘的行为信任控制 [J]. 华南理工大学学报：自然科学版, 2009, 37 (5): 94-100.

[11] 田立勤. 网络用户行为的安全可信分析与控制 [M]. 北京：清华大学出版社, 2011: 144-152.

[12] 魏中强，徐宏喆，李文，等. 基于最大信息系数的贝叶斯网络结构学习算法 [J]. 计算机应用研究, 2014, 31 (11): 3261-3265.

[13] 王晓菊，田立勤，赵竞雄. 基于物联网的用户行为认证机制与分析 [J]. 南京理工大学学报：自然科学版, 2015, 39 (1): 70-77.

[14] Tang H, Mantao W. User identity authentication based on the combination of mouse and keyboard behavior [J]. International Journal of Security and Its Applications, 2016, 10 (6): 29-36.

[15] 慕春棣，叶俊. 基于数据挖掘的贝叶斯网络 [J]. 软件学报, 2000, 11 (5): 660-666.

[16] Abramson M, Aha D W. User authentication from Web browsing behavior [C]// Proc of FLAIRS Conference. 2014.

[17] Tian L Q, Lin C, Ni Y. Evaluation of user behavior trust in cloud computing [C]// Proc of IEEE International Conference on Computer Application and System Modeling. 2010: V7-567-V7-572.

[18] 冯登国，张敏，张妍，等. 云计算安全研究 [J]. 软件学报, 2011, 22 (1): 71-83.

[19] Goel N K, Jha C. Analyzing users behavior from Web access logs using automated log analyzer tool [J]. International Journal of Computer Applications, 2013, 62 (2): 29-33.

[20] Brosso I, Neve A L, Bressan G, et al. A continuous authentication system based on user behavior analysis [C]// Proc of IEEE Ares'10 International Conference on Availability, Reliability, and Security. 2010: 380-385.